C'est très CHIC: A compact password-authenticated key exchange from lattice-based KEM

Afonso Arriaga[1], Manuel Barbosa[2], Stanislaw Jarecki[3], and Marjan Škrobot[1]

[1] SnT - University of Luxembourg
{afonso.delerue, marjan.skrobot}@uni.lu
[2] University of Porto (FCUP), INESC-TEC
and Max Planck Institute for Security and Privacy
mbb@fc.up.pt
[3] University of California at Irvine
stanislawjarecki@gmail.com

Abstract. Driven by the NIST's post-quantum standardization efforts and the selection of Kyber as a lattice-based Key-Encapsulation Mechanism (KEM), several Password Authenticated Key Exchange (PAKE) protocols have been recently proposed that leverage a KEM to create an efficient, easy-to-implement and secure PAKE. In two recent works, Beguinet et al. (ACNS 2023) and Pan and Zeng (ASIACRYPT 2023) proposed generic compilers that transform KEM into PAKE, relying on an Ideal Cipher (IC) defined over a group. However, although IC on a group is often used in cryptographic protocols, special care must be taken to instantiate such objects in practice, especially when a low-entropy key is used. To address this concern, Dos Santos et al. (EUROCRYPT 2023) proposed a relaxation of the IC model under the Universal Composability (UC) framework called Half-Ideal Cipher (HIC). They demonstrate how to construct a UC-secure PAKE protocol, EKE-KEM, from a KEM and a modified 2-round Feistel construction called m2F. Remarkably, the m2F sidesteps the use of an IC over a group, and instead employs an IC defined over a fixed-length bitstring domain, which is easier to instantiate.

In this paper, we introduce a novel PAKE protocol called CHIC that improves the communication and computation efficiency of EKE-KEM, by avoiding the HIC abstraction. Instead, we split the KEM public key in two parts and use the m2F directly, without further randomization. We provide a detailed proof of the security of CHIC and establish precise security requirements for the underlying KEM, including one-wayness and anonymity of ciphertexts, and uniformity of public keys. Our findings extend to general KEM-based EKE-style protocols and show that a passively secure KEM is not sufficient. In this respect, our results align with those of Pan and Zeng (ASIACRYPT 2023), but contradict the analyses of KEM-to-PAKE compilers by Beguinet et al. (ACNS 2023) and Dos Santos et al. (EUROCRYPT 2023).